HT2026 Groups & Group Actions Lecture Notes

Remaining TODOs: 1

Contents

1. Groups

Definition 1.1: Let S be a set. A binary operation on S is a function $* : S \times S \to S$.

We define $a * b := *(a, b)$.

Remark: If $*$ is understood implicitly, we often write ab for $a * b$.

Definition 1.2: $*$ admits an identity element if $\exists e \in S$ s.t. $a * e = a = e * a \ \forall a \in S$.

Definition 1.3: Suppose that e is an identity element, then inverses exist for $(S, *)$ if $\forall a \in S \ \exists b \in S$ s.t. $a * b = e = b * a$.

Definition 1.4: A group is a pair $(G, *)$ where $* : G \times G \to G$ is a binary operation which is associative, admits an identity, and for which inverses exist.

Definition 1.5: G is an abelian group if $*$ is commutative.

Lemma 1.6: Let $*$ be a binary operation on S.
(a) If e_1, e_2 are identity elements, then $e_1 = e_2$.
(b) If $e \in S$ is an identity element, $a \in S$, $*$ is associative, and b_1, b_2 are inverses of a under $*$, then $b_1 = b_2$.

Proof:
(a) $e_1 = e_1 * e_2 = e_2$

(b)
$$\begin{aligned} b_1 &\overset{\text{(id)}}{=\!=} b_1 * e \\ &\overset{\text{(inv)}}{=\!=\!=} b_1 * (a * b_2) \\ &\overset{\text{(assoc)}}{=\!=\!=\!=} (b_1 * a) * b_2 \\ &\overset{\text{(inv)}}{=\!=\!=} e * b_2 \\ &\overset{\text{(id)}}{=\!=} b_2 \end{aligned}$$

□

Definition 1.7: Let $(S, *)$ be a set with a binary operation, which admits inverses, then $\forall a \in S$, we write a^{-1} to mean the inverse of a.

Remark: $-a$ is also commonly used to denote the inverse of a if $(S, +)$ is an abelian group.

Example (symmetry group):

Definition 1.8: Let $\mathrm{Sym}(X) := \{f : X \to X \mid f \text{ bijective}\}$.

Proposition 1.9: $(\mathrm{Sym}(X), \circ)$ is a group.

Proof: Suppose f, g are bijections. Then:

- $f \circ g$ is injective:

$$\begin{aligned} & (f \circ g)(x) = (f \circ g)(y) \\ \implies & f(g(x)) = f(g(y)) \\ \implies & g(x) = g(y) \\ \implies & x = y \end{aligned}$$

- $f \circ g$ is surjective:

$$\begin{aligned} & \forall x \in X, \exists y \in X \text{ s.t. } z = f(y) \\ & \exists x \in X \text{ s.t. } y = g(x) \\ \implies & z = f(g(x)) = (f \circ g)(x). \end{aligned}$$

So $f \circ g$ is a bijection, and $f \circ g$ is a binary operation on $\mathrm{Sym}(x)$.

Composition is associative.

We have an identity, $\mathrm{id}_X : X \to X; x \mapsto x$, which satisfies $f \circ \mathrm{id}_x = f = \mathrm{id}_X \circ f$, $\forall f \in \mathrm{Sym}(f)$.

We have inverses: $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$. □

Definition 1.10: If $X = \{1, 2, ..., n\}$, $S_n := \mathrm{Sym}(X)$ is the nth symmetric group.

Remark: $\mathrm{Sym}(X)$ can also be interpreted as the permutations of X.

Example (fields):

Let $(F, +, \times)$ be a field.

Then $(F, +)$ is an abelian group, with identity element 0_F, whereas $(F \setminus \{0_F\}, \times)$ (sometimes denoted F^*) is also an abelian group with identity element 1_F.

For example, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ all form groups under addition, or under multiplication when zero is excluded.

Also $\mathbb{Z}_p^*$:= non-zero integers mod p, for prime p, is a group under multiplication.

Example (matrices):

$(M_n(F), +)$ is an abelian group (where $M_n(F)$ is the set of $n \times n$ matrices over F).

Definition 1.11: $GL_n(F) := \{A \in M_n(F) \mid \det A \neq 0\}$.

$(GL_n(F), \cdot)$ is the nth general linear group over F.

Let $SL_n(F) := \{A \in GL_n(F) \mid \det A = 1\}$; this is the nth standard linear group over F under matrix multiplication.

Example:

Definition 1.12: Let X be a set, let $Y \subseteq X$.

Let $\mathrm{Stab}(Y) := \{f \in \mathrm{Sym}(X) : f(Y) = Y\}$.

Proposition 1.13: $(\mathrm{Stab}(Y), \circ)$ is a group.

Proof: Necessary to prove: $\forall f, g \in \mathrm{Stab}(Y), f \circ g \in \mathrm{Stab}(Y)$: $(f \circ g)(Y) = f(g(Y)) = f(Y) = Y$.

Associativity is inherited from the symmetric group.

$\mathrm{id}_X(Y) = Y \implies \mathrm{id}_X \in \mathrm{Stab}(Y)$.

Let $f \in \mathrm{Stab}(Y)$, then $f(Y) = Y$. Hence $f^{-1}(f(Y)) = Y$, and $f^{-1}(f(Y)) = f^{-1}(Y)$, so $f^{-1} = Y$, so $f^{-1} \in \mathrm{Stab}(Y)$. □

Definition 1.14: $(\mathrm{Stab}(Y), \circ)$ is the stabiliser subgroup.

Definition 1.15: Let G be a group, with binary operation $*$. A subset $H \subseteq G$ is a subgroup if $*$ restricts to a map $* : H \times H \to H$ which then makes $\left(H, *_{/H}\right)$ into a group. We write $H \leq G$.

Example: $(\mathbb{R}, +) \leq (\mathbb{C}, +)$

Proposition 1.16 (Subgroup Test): Let G be a group. A subset H of G is a subgroup iff :

(i) $e \in H$

(ii) $\forall x, y \in H,\ xy^{-1} \in H$

Proof:

"$\Longrightarrow$":

Assume H is a subgroup of G. Then H is closed under multiplication and inversion. Therefore $\forall x, y \in H,\ xy^{-1} \in H$ and also $e \in H$.

"$\Longleftarrow$": Associativity on H is inherited from G.

(i) $\Longrightarrow e \in H$.

Apply (ii) with $x = e$, giving $\forall y \in H, y^{-1} \in H$.

So $\left(H, *_{/H}\right)$ is a group. □

Example: Let $G = GL_n(\mathbb{R})$.

Let $O(n) = \{\mathbf{A} \in G \mid \mathbf{A}^\top \mathbf{A} = \mathbf{I}\}$, the orthogonal matrices.

(i) $\mathbf{I}^\top \mathbf{I} = \mathbf{I} \Longrightarrow \mathbf{I} \in O(n)$.

(ii) $\mathbf{A}, \mathbf{B} \in O(n) \Longrightarrow (\mathbf{AB}^{-1})^\top (\mathbf{AB}^{-1}) = (\mathbf{B}^{-1})^\top \mathbf{A}^\top \mathbf{AB}^{-1}$

$$
\begin{aligned}
&= (\mathbf{B}^{-1})^\top \mathbf{B}^{-1} \\
&= (\mathbf{B}^\top)^{-1} \mathbf{B}^{-1} \\
&= (\mathbf{BB}^\top)^{-1} \\
&= \mathbf{I}^{-1} \quad (\mathbf{B}^\top \mathbf{B} = \mathbf{I} \Longrightarrow \mathbf{BB}^\top = \mathbf{I} \text{ for square } \mathbf{B}) \\
&= \mathbf{I}
\end{aligned}
$$

Hence by the subgroup test, $O(n) \leq GL_n(\mathbb{R})$.

Also $SL_n(F) \leq GL_n(F)$ can be shown by the subgroup test.

Lemma 1.17: If $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.

Corollary 1.18: $SO(n) = SL_n(\mathbb{R}) \cap O(n) \leq GL_n(\mathbb{R})$.

Definition 1.19: Let $(G, *_G), (H, *_H)$ be groups.

The product group is $(G \times H, *_{G\times H})$, where $(g_1, h_1) *_{G\times H} (g_2, h_2) = (g_1 *_G g_2,\ h_1 *_H h_2)$.

Lemma 1.20: The product of two groups is a group.

Proof: Associativity is easy.

$(g, h)\ (e, e) = (ge, he) = (g, h) = (e, e)\ (g, h)$, so (e, e) is an identity.

The inverse of (g, h) is (g^{-1}, h^{-1}). □

Definition 1.21: Let G be a group. G is cyclic if $\exists g \in G$ s.t. $G = \{g^n \mid n \in \mathbb{Z}\}$, where

$$g^n = \begin{cases} gg^{n-1} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ (g^n)^{-1} & \text{if } n < 0. \end{cases}$$

g is known as a generator of G.

Example:

Definition 1.22: $G = (\mathbb{Z}, +)$ is a cyclic group with $g = 1$.

This is the infinite cyclic group.

Definition 1.23: For $n \in \mathbb{Z}_{>0}$, $C_n = \{e, g, g^2, ..., g^{n-1}\}$ is a cyclic group with binary operation

$$g^a g^b = \begin{cases} g^{a+b} & \text{if } a + b \leq n - 1 \\ g^{a+b-n} & \text{if } n \leq a + b \leq 2n - 2 \end{cases}$$

and inverse $(g^a)^{-1} = g^{n-a}$ for $0 \leq a < n$. C_n is the cyclic group of order n.

Remark: A cyclic group can have more than one generator; for instance, $(\mathbb{Z}, +)$ also has -1 as a generator.

Remark: $C_5 = \langle g^2 \rangle$, where, for $h \in H$, we write $\langle h \rangle \coloneqq \{h^n \mid n \in \mathbb{Z}\}$. This is because 2 and 5 are coprime.

Definition 1.24: An isometry $T : \mathbb{R}^n \to \mathbb{R}^n$ is a distance-preserving function, i.e. $|T(\boldsymbol{v}) - T(\boldsymbol{w})| = |\boldsymbol{v} - \boldsymbol{w}|$ for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^n$.

Remark: By the subgroup test, $\mathrm{Isom}(\mathbb{R}^n) \leq \mathrm{Sym}(\mathbb{R}^n)$.

Remark: $\forall T \in \mathrm{Isom}(\mathbb{R}^n), \exists! \mathbf{A} \in O(n), \boldsymbol{b} \in \mathbb{R}^n$ s.t. $T(\boldsymbol{v}) = \mathbf{A}\boldsymbol{v} + \boldsymbol{b}$ for all $\boldsymbol{v} \in \mathbb{R}^n$.

Definition 1.25: Let $n \in \mathbb{Z}_{>0}$. Let P_n be the regular n-sided polygon centred at the origin O.

The dihedral group D_{2n} is

$$D_{2n} \coloneqq \mathrm{Isom}(\mathbb{R}^2) \cap \mathrm{Stab}(P_n);$$

that is, it is the group of distance-preserving transformations that stabilise the regular n -sided polygon centred at the origin.

We denote the rotation by $2\pi/n$ anticlockwise by r, and the reflection in an axis (which one depends on which way we choose to draw the polygons) by s. Then the elements of D_{2n} are $e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s$. Note that this is $2n$ elements.

Proposition 1.26: $S_{2n} = \{r^i s^j \mid 0 \leq i < n, j \in \{0, 1\}\}$.

Proof: Suppose $r^i s^j = r^a s^b$ w.l.o.g. $i \geq a$. Then $r^{-a} r^i s^j = r^{-a} r^a s^b = s^b$, so w.l.o.g. $a = 0$.

If $j = b$, then $r^i = r^0 = e \implies r^i(p_0) = e(p_0)$ for some point p_0, so $i = 0$.

If $j \neq b$, $r^i = s$. Take dets to get $1 = -1$, contradiction.

Now let $P \in D_{2n}$. Then $P(p_0) = p_i = r^i(p_0)$ for some $i \in \{0, ..., n-1\}$.

Hence $r^{-i}P(p_0) = p_0$.

Now $\left|r^{-i}P(p_1) - r^{-i}P(p_0)\right| = |p_1 - p_0|$, hence $r^{-i}P(p_1) \in \{p_1, p_{n-1}\}$.

TODO finish this off □

Definition 1.27: The order of a group G is $|G|$, the number of elements in G.

Definition 1.28: If $G = \{g_1, ..., g_n\}$, its Cayley table is an $n \times n$ array where with $g_i g_j$ in the ith row and jth column.

Definition 1.29: Let G, H be groups. An isomorphism between G and H is a bijection $\varphi : G \to H$ s.t.

$$\varphi(g_1 g_2) = \varphi(g_1)\ \varphi(g_2).$$

If there is an isomorphism between G and H, then G and H are isomorphic, written $G \cong H$.

Remark: Isomorphic finite groups will have the "same" Cayley tables (up to row/column orders).

Definition 1.30: For a group G, the order of an element $g \in G$ is

$$o(g) := \min\{r \in \mathbb{Z}_{>0} \mid g^r = e\}.$$

If $g^r \neq e$ for all $r \in \mathbb{Z}_{>0}$, we say that g has infinite order.

Lemma 1.31: If $\varphi : G \to H$ is an isomorphism, then $\forall g \in G$,

$$o(\varphi(g)) = o(g).$$

Proof:

First we show that $\varphi(e) = e$:

$$\begin{aligned} \varphi(e) &= \varphi(e^2) \\ &= \varphi(e)^2 \\ \implies e &= \varphi(e)^{-1}\varphi(e) \\ &= \varphi(e)^{-1}\varphi(e)^2 \\ &= \varphi(e). \end{aligned}$$

Then

$$\begin{aligned} g^r = e &\iff \varphi(g^r) = \varphi(e) = e \\ &\iff \varphi(g)^r = e. \end{aligned}$$

Hence

$$\begin{aligned} o(g) &= \min\{r > 0 \mid g^r = e\} \\ &= \min\{r > 0 \mid \varphi(g)^r = e\} = o(\varphi(g)). \end{aligned}$$

□

2. Permutation groups

Remark: $|S_n| = n!$.

Remark: We write permutations on the right, i.e. if $i \in \{1, ..., n\}, \sigma \in S_n$, then $i\sigma := \sigma(i)$.

This means that composition is backwards from the usual order.

Definition 2.1: A cycle is a permutation $\sigma \in S_n$ such that $\exists \{a_1, ..., a_m\} \subseteq \{1, ..., n\}$ s.t. $a_k\sigma = a_{k+1}$ for $k \in \{1, ..., m-1\}$ and $a_m\sigma = a_1$, and for all $x \in \{1, ..., n\} \setminus \{a_1, ..., a_m\}$, $x\sigma = x$.

We denote this cycle as $(a_1\ a_2\ ...\ a_m)$.

Remark: We could denote $e = (1)(2)\cdots(n)$.

Lemma 2.2: Disjoint cycles commute.

Proof: Let $\sigma = (a_1\ ...\ a_m)$ and $\tau = (b_1\ ...\ b_k)$ be disjoint cycles, i.e. $\{a_1, ..., a_m\} \cap \{b_1, ..., b_k\} = \varnothing$.

Let $i \in \{1, ..., n\}$. Then

$$i\sigma\tau = \begin{cases} a_{j+1}\tau = a_{j+1} & \text{if } i = a_j \\ i\tau = b_{j+1} & \text{if } i = b_j \\ i & \text{otherwise;} \end{cases}$$

$$i\tau\sigma = \begin{cases} i\sigma = a_{j+1} & \text{if } i = a_j \\ b_{j+1}\sigma = b_{j+1} & \text{if } i = b_j \\ i & \text{otherwise.} \end{cases}$$

□

Theorem 2.3: Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

Moreover, this factorisation is unique up to cycling of elements within cycles, and order of (commuting) factors.

Index